UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,858	09/05/2003	Sonia Reed	016222-012810US	8576

20350 7590 04/29/2008

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
DWIVEDI, MAHESH H	

ART UNIT	PAPER NUMBER
2168	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/656,858
Filing Date: September 05, 2003
Appellant(s): REED ET AL.

Patrick J. Jewik
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02/04/2008 appealing from the Office action mailed 06/06/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims in the brief is correct.

(4) Status of Amendments After Final

The after-final amendments filed concurrently with the instant appeal on 02/04/2008 are entered into record.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,970,891	Deo et al.	11/29/2005
5,649,118	Carlisle et al.	07/15/1997

6,880,084 Brittenham et al. 04/12/2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Deo et al.** (U.S. Patent 6,970,891) and in view of **Carlisle et al.** (U.S. Patent 5,649,118).

4. Regarding claim 13, **Deo** teaches a system comprising:

A) a client having a plurality of applications residing thereon (Column 3, lines 44-54); and

B) a secure token having a storage architecture (Column 6, lines 27-34), wherein the storage architecture includes:

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

F) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and
G) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).
H) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
I) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
J) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"a client having a plurality of applications residing thereon"** as "The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)" (Column 3, lines 49-54). The examiner further notes that **Deo** teaches **"a secure token having a storage architecture"** as "With this architecture, volatile data kept in volatile memory is no longer bound to a single application, but can be accessed by multiple applications" (Column 6, lines 27-29). The examiner further notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under**

each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

C) a directory and one or more attributes associated with the directory;

E) one or more cell groups under the directory each cell group having one or more associated attributes;

K) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;

L) wherein the client terminal is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30), **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the

respective users" (Column 6, lines 30-51), and **"wherein the client terminal is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 14, 33, and 52, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes permit a first set of operations by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

B) wherein the one or more attributes permit a second set of by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

C) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"wherein the one or more attributes permit a first set of operations by a first application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit a second set of by a second application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining

which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A, B) associated with the directory.

Carlisle, however, teaches **"associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 16, 35, 51, and 54, **Deo** further teaches a system comprising:

A) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

B) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

C) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Regarding claims 17, 36, and 55, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the secure token is a smart card (Column 1, lines 6-8).

The examiner notes that **Deo** teaches **"wherein the secure token is a smart card"** as "This invention relates to integrated circuit (IC modules, such as smart cards" (Column 1, lines 6-7).

Regarding claims 19, 38, and 57, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the secure token is a static or native smart card (Column 3, lines 44-54).

The examiner notes that **Deo** teaches **"wherein the secure token is a static or native smart card"** as "The operating system 114 includes a file system 118 that manages files stored on the smart card" (Column 3, lines 44-45).

Regarding claim 20, **Deo** teaches a secure token comprising:

B) wherein the one or more attributes are used to control access by the plurality of applications associated with a client (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

F) wherein the one or more attributes permit a first application to access after a first access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

G) wherein the one or more attributes permit a second application to access after a second access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

H) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications associated with a client"** as "an access control list (ACL) can be associated…gain access to and perform file

operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit a first application to access after a first access condition is satisfied"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit a second application to access after a second access condition is satisfied"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or

applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A) a directory and one or more attributes associated with the directory;

C, F, G) one or more cell groups under the directory each cell group having one or more associated attributes;

I) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;

J) wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's

HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 21, and 40, **Deo** further teaches a secure token and method comprising:

A) wherein the one or more attributes permit access to one application and deny access to another application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit access to one application and deny access to another application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4).

Deo does not explicitly teach:

A) associated with the directory.

Carlisle, however, teaches **"associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 23 and 42, **Deo** further teaches a secure token and method comprising:

A) wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44).

The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42).

Regarding claims 24, and 43 **Deo** further teaches a secure token and method comprising:

A) wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder (Column 7, lines 55-67).

The examiner further notes that **Deo** teaches **"wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure**

token to a token holder" as "ScwCreateDir Creates a directory with the given access control list (ACL) file" (Column 7, lines 57-58)

Regarding claims 25, and 44, **Deo** does not explicitly teach a secure token and method comprising:

A) wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token holder.

Carlisle, however, teaches **"wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token holder"** as "First, O, controls the establishment of a service provider's directory" (Column 14, lines 63-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 26, and 45, **Deo** does not explicitly teach a secure token and method comprising:

A) wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder.

Carlisle, however, teaches **"wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder"** as "First, O, controls the establishment of a service provider's directory…through the operating system's design, O can control the amount of memory that each service provider has access to, and thus can control the number of service providers that can "coexist" on a smart card"" (Column 14, lines 63-67-Column 15, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Carlisle's would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 27, and 46, **Deo** further teaches a secure token and method comprising:

A) wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder (Column 6, lines 62-67).

The examiner notes that Deo teaches **"wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder"** as "At block 304, in response to a request from an authorized application to create or open a file, the file system 118 creates or opens a file and obtains a handle to that file" (Column 6, lines 62-67).

Regarding claims 28, and 47, **Deo** further teaches a secure token and method comprising:

A) wherein the one or more attributes associated are modified in terms of permitting or denying access by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **"wherein the one or more attributes associated with the directory are modified in terms of permitting or denying access to the directory by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

Deo does not explicitly teach:

A) with the directory.

Carlisle, however, teaches **"with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Carlisle's would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 30, and 49, **Deo** further teaches a secure token and method comprising:

A) wherein the one or more attributes associated with the cell are modified in terms of permitting or denying access to that cell by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **"wherein the one or more attributes associated with the cell are modified in terms of permitting or denying access to that cell by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

Regarding claims 31, and 50, **Deo** further teaches a secure token, and method comprising:

A) wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **"wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

Regarding claim 32, **Deo** teaches a secure token comprising:

B) wherein the one or more attributes are used to control access by the plurality of applications associated with a client terminal (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and
E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).
F) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
G) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
H) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications associated with a client terminal"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or**

more attributes associated with a cell are used to control access to that cell by the plurality of applications" as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A) a directory and one or more attributes associated with the directory;
C) one or more cell groups under the directory each cell group having one or more associated attributes;
I) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;
J) wherein the client terminal is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client terminal is**

adapted to use the passcode or key to access data in the directory, cell group, or cell" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claim 39, **Deo** teaches a method comprising:

B) wherein the one or more attributes are used to control access by the plurality of applications associated with a client (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

F) wherein the one or more attributes permit a first application to access after a first access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

G) wherein the one or more attributes permit a second application to access after a second access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

H) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications associated with a client"** as

"an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit a first application to access after a first access condition is satisfied"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit a second application to access after a second access condition is satisfied"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the first access condition is different from the second access condition"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list)

table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A) providing a directory and one or more attributes associated with the directory;

C, F, and G) providing one or more cell groups under the directory each cell group having one or more associated attributes;

I) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;

J) wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"providing a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"providing one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of

the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claim 48, **Deo** further teaches a method comprising:

A) wherein the one or more attributes associated are modified in terms of permitting or denying access by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **"wherein the one or more attributes associated with a cell group are modified in terms of permitting or denying access to that cell group by the plurality of applications"** as "the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files" (Column 4, lines 37-44).

Deo does not explicitly teach:

A) with the cell group.

Carlisle, however, teaches **"with the cell group"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Carlisle's would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claims 58 and 61, **Deo** does not explicitly teach a method and secure token comprising:

A) wherein the first application is associated with a first party and the second application is associated with a second party; and

B) wherein the first and the second party have an existing business relationship; and

C) agree to share data on the secure token according to agreed security controls.

Carlisle, however, teaches **"wherein the first application is associated with a first party and the second application is associated with a second party"** as "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19), **"wherein the first and the second party have an existing business relationship"** as "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a

particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19), and **"agree to share data on the secure token according to agreed security controls"** as "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching

Carlisle's would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claim 59, **Deo** does not explicitly teach a method comprising:
A) wherein the first application or the second application is a loyalty application.

Carlisle, however, teaches **"wherein the first application or the second application is a loyalty application"** as "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Regarding claim 60, **Deo** does not explicitly teach a method comprising:

A) wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups.

Carlisle, however, teaches **"wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups"** as "One aspect of the arrangement disclosed herein is that the smart card's issuer/owner (O) has a general knowledge of, and control over, the service providers whose "applications" are present on the smart card. First, O controls the establishment of a service provider's directory. Second, O can delete any directory at the holder's request, or whenever O gains access the smart card (with, or without, the holder's consent). Third, O is the only party who knows the identity of all the service providers who share the smart card, and various particulars about those service providers" (Column 14, lines 60-67-Column 15, lines 1-2) and "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical

levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

5. Claims 18, 37, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Deo et al.** (U.S. Patent 6,970,891) and in view of **Carlisle et al.** (U.S. Patent 5,649,118) as applied to claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61 and further in view of **Brittenham et al.** (U.S. Patent 6,880,084)

6. Regarding claim 18, **Deo** teaches a system comprising:

A) a client having a plurality of applications residing thereon (Column 3, lines 44-54); and

B) a secure token having a storage architecture (Column 6, lines 27-34), wherein the storage architecture includes:

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

F) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

G) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

H) wherein the secure token is a smart card (Column 1, lines 6-8).

The examiner notes that **Deo** teaches **"a client having a plurality of applications residing thereon"** as "The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)" (Column 3, lines 49-54). The examiner further notes that **Deo** teaches **"a secure token having a storage architecture"** as "With this architecture, volatile data kept in volatile memory is no longer bound to a single application, but can be accessed by multiple applications" (Column 6, lines 27-29). The

examiner further notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the secure token is a smart card"** as "This invention relates to integrated circuit (IC modules, such as smart cards" (Column 1, lines 6-7).

Deo does not explicitly teach:

C) a directory and one or more attributes associated with the directory;

E) one or more cell groups under the directory each cell group having one or more associated attributes;

J) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;

K) wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing

Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

I) wherein the smart card is an open platform smart card.

Brittenham, however, teaches **"wherein the smart card is an open platform smart card"** as "embodiments of the present invention may support Java Card (with

Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows" (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham's** would have allowed **Deo's** and **Carlisle's** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

Regarding claim 37, **Deo** teaches a secure token comprising:

B) wherein the one or more attributes are used to control access by the plurality of applications associated with a client (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

F) wherein the secure token is a smart card (Column 1, lines 6-8).

The examiner notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications associated with a client"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an

access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"wherein the secure token is a smart card"** as "This invention relates to integrated circuit (IC modules, such as smart cards" (Column 1, lines 6-7).

Deo does not explicitly teach:

A) a directory and one or more attributes associated with the directory;

C) one or more cell groups under the directory each cell group having one or more associated attributes;

H) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;

I) wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are **".profile"** file 11, **"passwd"** file 12, "log" file 17, "filex" file 13, "filey" file 14, and **"ID"** file 18. A number of subdirectories are also found below root, with each being used as the **"HOME"** directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG.

2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

G) wherein the smart card is an open platform smart card.

Brittenham, however, teaches **"wherein the smart card is an open platform smart card"** as "embodiments of the present invention may support Java Card (with Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows" (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham's** would have allowed **Deo's** and **Carlisle's** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

Regarding claim 56, **Deo** teaches a method comprising:

B) wherein the one or more attributes are used to control access by the plurality of applications associated with a client (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)
D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and
E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
F) wherein the secure token is a smart card (Column 1, lines 6-8).

The examiner notes that **Deo** teaches **"wherein the one or more attributes are used to control access by the plurality of applications associated with a client"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated…gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files…and the like" (Column 4, lines 37-42).

Deo does not explicitly teach:
A) providing a directory and one or more attributes associated with the directory;
C) providing one or more cell groups under the directory each cell group having one or more associated attributes.

H) wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key;
I) wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

Carlisle, however, teaches **"providing a directory and one or more attributes associated with the directory"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"providing one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30), **"wherein one or more attributes associated with the directory, cell group, or cell are associated with a passcode or key"** as "FIG. 2 illustrates a structure that responds to this sensitivity of service providers. According to the structure of FIG. 2, Root owns the root directory and any number of files (directory files or normal files) that it wishes to create. For example, FIG. 2 includes a root directory file 10 and below it there are ".profile" file 11, "passwd" file 12, "log" file 17, "filex" file 13, "filey" file 14, and "ID" file 18. A number of subdirectories are also found below root, with each being used as the "HOME" directory of a user (service provider), and also creates a password file for each such user HOME directory. For example, FIG. 2 includes a directory file 15, named "htb" (the smart card's Holder), a directory file 20 named "bankA", and a directory file 25 named "airlineA". Each one of the directories includes a "passwd" file (16, 21, and 26, respectively) below the associated user's HOME directory, as well as a ".profile" file. This placing of the password files has some advantages but it is not a requirement. Importantly, ownership of each such password files is assigned to the user associated with that file and the directory above it. It may also be advantageous to grant ownership of files (directories) 15, 20 and 25 to the respective users" (Column 6, lines 30-51), and **"wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory…only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

G) wherein the smart card is an open platform smart card.

Brittenham, however, teaches **"wherein the smart card is an open platform smart card"** as "embodiments of the present invention may support Java Card (with Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows" (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham's** would have allowed **Deo's** and **Carlisle's** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

(10) Response to Argument

A. Claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Deo et al.** (U.S. Patent 6,970,891) and in view of **Carlisle et al.** (U.S. Patent 5,649,118).

Arguments (1): Regarding Independent Claims 13 and 39, Appellant argues that "While the passage cited by the Examiner mentions "nonresident applications," such nonresident applications are "downloaded" to the memory 106 in a smartcard. The passage cited by the Examiner does not state or suggest that there is any "client" having a plurality of applications residing thereon. Deo et al.'s smart card cannot be the "client", since Deo et al.'s smart card is allegedly a "secure token." Consequently, obviousness has not been established for this reason alone".

However, according to the limitations in independent claims 13 and 39, the limitation merely states that "a client having a plurality of applications residing thereon". Furthermore, the examiner wishes to point to Column 3 of **Deo** which states "**One or**

more applications 112 and an operating system 114 are stored in ROM 108. Some applications as well as parts of the operating system can reside in EEPROM as well. When the smart card is coupled to a card reader and receives power, the application(s) 112 and operating system 114 are executed on the processor 102. The operating system 114 exposes a set of application program interfaces (APIs) that enable resident applications 112 to perform tasks and manipulate data on the smart card. In addition, **one or more nonresident applications 116, which execute external to the smart card (e.g., programs on kiosks, point-of-purchase machines, etc.)**, may also place function calls with the operating system 114 to perform tasks or manipulate data on the smart card. Examples of such tasks include access security, cryptographic functions (e.g., encryption, decryption, signing, and verification), file management, commerce, and so forth. One suitable operating system is the "Windows for Smart Card" operating system from Microsoft Corporation" (Column 3, lines 25-43) and "The volatile files 122 make it possible for **multiple resident applications 112**, as well **as nonresident applications 116** that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)" (Column 3, lines 49-54). The examiner further wishes to state that it is clear that **Deo** teaches multiple applications residing on a client (see "**One or more applications 112** and an operating system 114 are stored in ROM 108" and "**one or more nonresident applications 116, which execute external to the smart card (e.g., programs on kiosks, point-of-purchase machines, etc.)**"). Moreover, because **Deo** teaches that the nonresident applications can be more than one from a kiosk (i.e. client), then as a result, **Deo** teaches the client having multiple applications residing on a secure token.

Arguments (2): Regarding Independent Claims 13 and 39, Appellant argues that "Obviousness has not been established, since the modifying Deo et al. in the manner proposed by the Examiner would be contrary to the intended purpose of Deo et al.'s smartcard subsystem. Deo et al. fails to teach or suggest at least the following limitation from independent claim 13: "wherein the one ore more attributes associated with the directory...or cell". Independent claim 39 recites a similar limitation" and "Passcodes and keys are not taught, suggested, or desired in Deo et al. Contrary to the

Examiner's allegation, there is no reason to modify Deo et al. to include passcodes or keys".

However, the cited art of **Carlisle** is used to teach the aforementioned limitations. Moreover, in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Furthermore, In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation for combing **Carlisle** with **Deo** is stated as to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62). Moreover, because both **Deo** and **Carlisle** deal with security on smartcard systems, they can be combined to teach aforementioned instant invention.

In addition, appellants argue that "If one were to modify Deo et al. to include passcodes and keys as alleged by the Examiner, this would render an essential part of Deo et al.'s system (i.e. the file system 118 and its associated access control mechanism) obsolete. As explained at col. 3, line 44 to col. 4, line 7 of Deo et al., the file system 118 is essential to the operation of Deo et al.'s smartcard and resides inside of he smartcard. If one were to modify Deo et al. to include a client with a plurality of applications and that uses passcodes or keys to access data on a secure token, there would be no need for Deo et al.'s file system 118 and its access control mechanism, since access to directories, cell groups, and cells would already be restricted. Consequently, there is no reason to modify Deo et al. to arrive at the pending claims,

since doing so would be contrary to the intended purpose of Deo et al's proposed invention".

However, as earlier discussed, **Deo** teaches a client have multiple applications residing on a secure token. Furthermore, the cited portions of **Deo** that the appellant alleges represents the purpose of **Deo**, in fact do not represent such a purpose. The cited passages merely describe the capabilities of the file system of **Deo's** smart card, and specifically how it deals with security. The modification of **Deo's** system via the addition of **Carlisle's** system would allow for additional access control capabilities via such passcodes and/or keys. Such a combination would be implanted from a motivation of providing for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62). Because **Deo** does not explicitly teach the claimed folders/directories of the instant invention, the inclusion of **Carlisle** would enable **Deo** to provide security control for hierarchal storage units stored on smart card (i.e. directories).

In addition, appellants argue that "Appellants submit that the Examiner's response does not address Appellant's argument that one would not have modified Deo et al. with the teachings of Carlisle et al., because doing so...for its intended purpose".

However, the examiner wishes to state that there was such a response to appellant's arguments in that the motivation to combine **Deo** with **Carlisle** would have allowed to ability control access to directories or sub-folders on a smart card. Because **Deo** is directed only to applications/files, **Carlisle's** security-based approach to directories does not destroy the purpose of **Deo**.

In addition, appellants argue that "Deo et al. does not state or suggest that Deo et al.'s access control mechanism is deficient in any way, so it is unclear why one skilled in the art would have modified Deo et al.'s system with passcodes or keys as alleged by the Examiner. Accordingly, Appellants maintain that one would not have been led t modify Deo et al. in the manner proposed by the Examiner and that obviousness has not been established".

However, because **Deo** is only directed toward security of applications/files, the inclusion of **Carlisle** allows **Deo** to teach security via passcodes/keys to directories/folders of such files. Thus, the modification of **Deo's** system via the addition of **Carlisle's** system would allow for additional access control capabilities via such passcodes and/or keys. Such a combination would be implanted from a motivation of providing for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62). Because **Deo** does not explicitly teach the claimed folders/directories of the instant invention, the inclusion of **Carlisle** would enable **Deo** to provide security control for hierarchal storage units stored on smart card (i.e. directories). Therefore, the combination of **Deo** and **Carlisle** is proper.

Arguments (3): Regarding Independent Claims 13 and 39, Appellant argues that "Obviousness has not been established, since the Examiner's proposed reason to combine is not in the prior art" and "Contrary to the Examiner's allegation, column 1, lines 59-62 does not state that passocdes and keys are necessary to provide access control at "higher" hierarchical levels. In fact, contrary to the Examiner's allegation, Carlisle et al. actually teaches away from providing access control at "higher" hierarchical levels. Carlisle et al. describes a variation on a UNIX operating system that restricts access to directories under the root directory to specific users. In this way, the control of each directory is provided to lower hierarchical levels, and not higher hierarchical levels as the Examiner alleges".

However, in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation for combing **Carlisle** with **Deo** is stated as to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access

to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62). Moreover, the examiner wishes to state that because **Carlisle** is directed towards security for directories/folders of multiple parties, the motivation to allow for security control on such directories/folders of multiple parties allows one to overcome the restriction of consumers by those parties. Moreover, because **Carlisle** teaches the use of passcodes/keys as a means for those security measures, then the motivation is proper. Furthermore, Applicants are also reminded that in order to disqualify a reference based on a "teach away" reasoning, the reference has to *explicitly* suggest or disclose the so-called teach away steps - Applicants assertion can not be accepted if it is unsupported by a valid evidence. In this case, the higher hierarchical levels are directed to folders (i.e. folders are higher than the files that are stored in them). Moreover, the reference to UNIX by appellant is appellant's own interpretation of the UNIX security system. The examiner's interpretation of allowing security control of higher levels, i.e. file to folder, does not represent "teach away" steps.

Arguments (4): Regarding Dependent Claim 58, Appellant argues that "Although this passage might suggest and "agreement" between two parties, Appellants submit that this passage does not describe an agreement to "share security controls." The word "security" is not remotely suggested in the cited passage. At best, the passage cited by the Examiner describes allowing a gasoline provider G to install an application on a smartcard, and allowing a bank B to be a provider of credit for gas sales to employee of A. There is no mention o suggestion of an agreement between any of the parties A, G, or B to "share security controls." Since each and every limitation of claim 58 is not taught or suggested by the cited art, obviousness has not been established".

However, according to the limitations in dependent claim 58, the limitations merely state that "wherein the first application is associated with a first party and the second application is associated with a second party; and wherein the first and the second party have an existing business relationship; agree to share data on the secure token according to agreed security controls". Furthermore, the examiner wishes to point to Columns 16-17 of **Carlisle** which state "It is quite possible for service providers to

form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19). The examiner further wishes to state no definition or explanation of what "share security controls" means is listed in the claim. As a result, the claim is entirely broad, and thus, the examiner the broadest reasonable interpretation of aforementioned limitation. Therefore, the gas provider's application, with its interaction with a Bank and a customer, broadly teaches the sharing of security controls.

In addition, appellant argues that "Obviousness has not been established, since the Examiner's proposed reason to modify Deo et al. with an "agreement to share security controls" does not have any rational underpinning" and "one would not have modified Deo et al. with an "agreement to share security controls" in order to provide "access control at higher hierarchal levels including subfolders and folders in order to restrict access to some providers on a smart card," as alleged by the Examiner, since an "agree[ment] to share data on the secure token according to agreed security controls" would not necessarily benefit from providing access control at higher hierarchical levels"

However, the examiner wishes to state that there would be a benefit to providing higher security measures with parties sharing security controls in that higher security controls would prevent rouge access to only intended applications.

In addition, appellants argue that "Actually, an "agreement to share security controls" allows additional access and does not further restrict access, so the Examiner's cited motivation providing access control at higher hierarchical levels actually teaches away from the modification proposed by the Examiner".

However, Applicants are also reminded that in order to disqualify a reference based on a "teach away" reasoning, the reference has to *explicitly* suggest or disclose the so-called teach away steps - Applicants assertion can not be accepted if it is unsupported by a valid evidence. In this case, there is not mention of not allowing shared security, so appellants arguments are completely unfounded.

Arguments (5): Regarding Dependent Claim 59, Appellant argues that "dependent claim 59 recites "wherein the first application or the second application is a loyalty application." Neither Deo et al. nor Carlisle et al. teaches or suggests this feature" and "The word "loyalty" is nowhere to be found in the passage cited by the Examiner. At best, the passage cited by the Examiner...Consequently, obviousness has not been established with respect to claim 59".

However, according to the limitations in dependent claim 59, the limitation merely states that "wherein the first application or the second application is a loyalty application". Furthermore, the examiner wishes to point to Columns 16-17 of **Carlisle** which state "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be

remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19). The examiner further wishes to state no definition or explanation of what a "loyalty application" means is listed in the claim. As a result, the claim is entirely broad, and thus, the examiner the broadest reasonable interpretation of aforementioned limitation. Therefore, the gas provider's application, with its interaction with a Bank and a customer, broadly teaches the loyalty application.

In addition, appellant argues that "Obviousness has not been established, since the Examiner's proposed reason to modify Deo et al. with a "loyalty application" does not have any rational underpinning. Here, the Examiner alleges that one would have modified Deo et al. with a "loyalty application" to provide…One would not have modified Deo et al. with a "loyalty application" in order to provide "access control at higher hierarchical levels including subfolders and folder in order to restrict access to some providers on a smart card" as alleged by the examiner, since a loyalty application would not necessarily benefit from providing access control at higher hierarchical levels. Since the rational that is used to modify Deo et al. does not have any rational underpinning, obviousness has been established with respect to claim 59.

However, the examiner wishes to state that the loyalty application is part of a hierarchal relationship with respect to access between owners and other parties, and as a result, the cited motivation is proper.

Arguments (6): Regarding Dependent Claim 60, Appellant argues that "dependent claim 59 recites "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups". Neither Deo et al. nor Carlisle et al. teaches or suggests this feature" and "The limitation "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups. Is nowhere to be found

in the passage cited by the Examiner. At best, the passage cited by the Examiner...obviousness has not been established with respect to claim 60".

However, the Examiner notes that the limitations are directed towards dependent claim 60 and not 59 as appellant alleges. Furthermore, according to the limitations in dependent claim 60, the limitation merely states that "wherein the first application can access only that cell group while the second application can access that cell group and additional cell groups". Furthermore, the examiner wishes to point to Columns 14-17 of **Carlisle** which state "One aspect of the arrangement disclosed herein is that the smart card's issuer/owner (O) has a general knowledge of, and control over, the service providers whose "applications" are present on the smart card. First, O controls the establishment of a service provider's directory. Second, O can delete any directory at the holder's request, or whenever O gains access the smart card (with, or without, the holder's consent). Third, O is the only party who knows the identity of all the service providers who share the smart card, and various particulars about those service providers" (Column 14, lines 60-67-Column 15, lines 1-2) and "It is quite possible for service providers to form cooperative alliances. Such alliances can specify various activities which are carried out in the smart cards whenever the smart card is accessed, or when the smart card is accessed by a particular user. The number of such possibilities is limitless, and the example below is merely illustrative. Assume, for example, that company A employs traveling salespeople who frequently need to purchase gasoline. A is likely to contract with O to issue a smart card for each of the salespeople (Holders) and request O to install A as a service provider and G as the gasoline provider. Sometime later, A may reach an agreement with bank B as a Provider of credit for the salespeople. That service can be remotely installed into all of the smart cards belonging to the salespeople by, for example, obtaining the cooperation of G. Specifically, A can request G to install a request for communication with O whenever a smart card interacts with G and found to have A as a user but not B as a user. All that G needs to do is modify the file that is executed when H logs in to communicate with G and direct the smart card to call O" (Column 16, lines 66-67-Column 17, lines 1-19). The examiner further wishes to state that the owner of

Carlisle's system clearly teaches the claimed second application that can access that cell group and additional cell groups since it "has a general knowledge of, and control over, the service providers whose "applications" are present on the smart card". Moreover, the service providers clearly teach the first application can access only that cell group. Therefore, the aforementioned limitations are taught by **Carlisle**.

In addition, appellant argues that "Obviousness has not been established, since the Examiner's proposed reason to modify Deo et al. with a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" does not have any rational underpinning" and "one would not have modified Deo et al. with an " first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" in order to provide "access control at higher hierarchical levels including subfolders and folder in order to restrict access to some providers on a smart card" because a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" would not necessarily benefit from providing access control at higher hierarchical levels.

However, the examiner wishes to state that there would be a benefit to providing higher security measures with applications that can multiple cell groups versus applications that can access only one cell group in that smart cards would have increased security to prevent rogue attacks.

In addition, appellants argue that "Actually, the proposed motivation to "restrict access" teaches away from a "first application [that] can access only that cell group while the second application can access that cell group and additional cell groups" since the first and second applications are sharing information in a cell group and access in not restricted between the application for that cell group. Thus, the Examiner's cited motivation actually teaches away from the modification proposed by the Examiner".

However, Applicants are also reminded that in order to disqualify a reference based on a "teach away" reasoning, the reference has to *explicitly* suggest or disclose the so-called teach away steps - Applicants assertion can not be accepted if it is

unsupported by a valid evidence. In this case, there is not mention of not allowing shared access, so appellants arguments are completely unfounded.

Arguments (7): Regarding claims 13, 20-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57-61, Appellant argues that "The rejection of claim 60 and other claims is based on improper hindsight" and "Clearly, it would not have been "obvious" for person of skill…are based on improper hindsight".

However, in response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Mahesh Dwivedi
Patent Examiner
AU 2168
/Mahesh H Dwivedi/
Examiner, Art Unit 2168

Tim Vo
Supervisory Patent Examiner
AU 2168
/Tim T. Vo/

Supervisory Patent Examiner, Art Unit 2168

Eddie Le

Appeals Practice Specialist

/Eddie C Lee/

Supervisory Patent Examiner, TC2100